Technical Report **1753**
September 1997

RMON-2 Implementation and Results for Common Operational Modeling, Planning, and Simulation Strategy During JWID 97

E. W. Jacobs
L. M. Gutman
R. H. Cheng
M. S. Lavelle

Naval Command, Control and Ocean Surveillance Center
RDT&E Division, San Diego, CA 92152–5001

Technical Report **1753**
September 1997

RMON-2 Implementation and Results for Common Operational Modeling, Planning, and Simulation Strategy During JWID 97

E. W. Jacobs
L. M. Gutman
R. H. Cheng
M. S. Lavelle

Naval Command, Control and Ocean Surveillance Center
RDT&E Division, San Diego, CA 92152–5001

NAVAL COMMAND, CONTROL AND OCEAN SURVEILLANCE CENTER
RDT&E DIVISION
San Diego, California 92152–5001

H. A. WILLIAMS, CAPT, USN
Commanding Officer

R. C. KOLB
Executive Director

ADMINISTRATIVE INFORMATION

The work detailed in this report was performed for the Networks Technology Branch (Code D827) Information Systems & Network Technology Division of the Communications Department (Code D80) of the Naval Command, Control and Ocean Surveillance Center (NCCOSC) RDT&E Division (NRaD). Funding was provided by Space and Naval Warfare Systems Command (SPAWAR PD 13, LCDR Glen Darling) under program element 0603794N. This report covers work performed mainly during Summer 1997.

Released by
R. L. Merk, Head
Networks Technology
Branch

Under authority of
R. J. Kochanski, Head
Information Systems
& Network Technology
Division

ACKNOWLEDGEMENTS

The authors wish to thank Chris Barber of MITRE Corp. for his ideas which led to the initiation of this project.

SB

EXECUTIVE SUMMARY

This report documents the results obtained from Remote Monitoring (RMON) technology in the Naval Command, Control and Ocean Surveillance Center RDT&E Division (NRaD) Common Operational Modeling, Planning, and Simulation Strategy (COMPASS) lab during the 1997 Joint Warrior Interoperability Demonstration (JWID 97). The report reviews the essentials of RMON and RMON-2 technology and describes COMPASS lab participation in JWID 97. The report then discusses the results of utilization of RMON-2 for operations and for historical data collection.

The operational utilization of RMON-2 in the COMPASS lab during JWID 97 was successful. The real-time information obtained from the RMON-2 probe and displayed using commercial off-the-shelf (COTS) software proved itself a necessary aid for network managers in maintaining desired network performance. The utilization of RMON-2 for collection of historical data was also successful. Data collection over the demonstration period documented the amount of traffic (octets and packets), the type of traffic (link layer through application layer protocols), and the source and destination of traffic (link and network layer addresses). For the purposes of the COMPASS lab participation in JWID 97, the historical data collection documented network utilization during the demonstration and helped explain network requirements for COMPASS in future scenarios. The type of historical data obtained during the demonstration would help in optimizing network performance in scenarios where the relevant networks will operate over extended time periods.

It is anticipated that the success of the implementation of RMON-2 in this demonstration will provide a stepping stone towards the utilization of this technology in the operational environment.

CONTENTS

Figures

1. INTRODUCTION

The Automated Integrated Communications System (AICS) is an advanced engineering program chartered to investigate the best ways of deploying commercial network management technologies in the Navy afloat networking environment and to determine the requirements and practices for adopting commercial network management to the Navy arena.

Briefly, network management is the monitoring and control of individual network resources (such as routers and links) and networks taken as a whole. Typical network management operations in the field are retrieving status and statistics, configuring network devices, and processing unsolicited messages by devices (e.g., alarms). The Remote Monitoring (RMON) standard provides an interface by which a network management application using the Simple Network Management Protocol (SNMP) directs the operation of stand-alone probes used to collect, collate, and report statistics on the packets traversing an attached network. The RMON standard, by in large, is concerned with the link-layer, e.g., Ethernet statistics. A recent extension, RMON-2, collects and collates statistics on protocols all the way up to the application layer. Thus, among the various kinds of network management functionality, RMON is concerned with the collection of network statistics.

AICS investigated RMON for the last 18 months with a view towards evaluating its effectiveness in an operational Navy afloat network. The effectiveness measures include: ease of use in an operational environment; the reliability of the data and implementations; and the timeliness and applicability of the statistical results to network performance management issues in an operational environment.

For the 1997 Joint Warrior Interoperability Demonstration (JWID 97), a RMON-2 probe was installed and utilized in the Common Operational Modeling, Planning, and Simulation Strategy (COMPASS) lab. Besides providing data points for the measures of effectiveness listed above, this experiment exposed engineers and managers of networking programs to the technology and gave them an opportunity to judge how well it might fit their systems. This paper reviews the operations and outcomes of that experiment.

The following section reviews RMON and RMON-2 technology. Section 3 provides an overview of JWID 97 and COMPASS and how RMON-2 was implemented in the COMPASS lab. Section 4 describes the results obtained using RMON-2 in the COMPASS lab during JWID 97, and section 5 provides a summary and conclusion.

2. RMON AND RMON-2 TECHNOLOGY

Remote network monitoring devices, often called monitors or probes, are instruments that aid in network management. A RMON probe consists of a) an interface that listens to a local area network (LAN) in a promiscuous mode and, b) an implementation of an SNMP agent supporting the the RMON management information base (MIB) or the RMON-2 MIB. Currently, RMON probes with Ethernet, token-ring, and Fiber Distributed Data Interface (FDDI) interfaces are available, although this document only discusses Ethernet RMON probes.

There are two RMON standards: RMON (reference 1) and an extension to RMON called RMON-2 (reference 2). These standards extend the information contained in the MIB-II standard (reference 3) and provide a far more detailed description of the traffic traveling on a LAN. RMON includes the capability to quickly access link layer (i.e., Ethernet layer) statistics. It also includes the capability to filter and selectively capture packets, thereby enabling analysis of higher network layers in a less convenient and less practical manner. The RMON-2 standard incorporates quick access to statistics all the way up to the application layer. Within the last 6 months COTS probes that conform to most of the RMON-2 standard have become available (reference 4). The RMON and RMON-2 MIBs describe the information that the probes maintain and make available to network management programs that issue appropriate SNMP requests. A RMON probe monitors only the LAN to which it is attached. It is called a *remote* network monitoring device because the information the probe collects can be retrieved remotely by management applications via SNMP requests. For general information on the SNMP manager/agent paradigm, see, for instance, reference 5.

To provide a better description of the type of information that can be obtained from a RMON probe, some of the groups in the RMON and RMON-2 MIBs are briefly described in the following paragraphs.

As described below, groups contained in the RMON MIB include the Ethernet statistics, history, host, hostTopN, matrix, filter, capture, alarm, and event groups.

Ethernet Statistic Group. This group contains statistics describing the Ethernet packets detected on the monitored LAN. These statistics include the number of Ethernet packets, octets, broadcast packets, multicast packets, cyclic redundancy code errors, fragments, jabbers, collisions, oversized packets, undersized packets, and packets of various sizes.

Ethernet History Group. The Ethernet history group records periodic statistical samples from an Ethernet LAN and stores them for later retrieval. This is useful in reducing the SNMP traffic between the SNMP management application and the probe in cases where they are separated by a busy or low-bandwidth link. A manager can use the history control group to configure the statistics collected in this group.

Host Group. The host group contains statistics associated with each Ethernet host discovered on the network. Contained in this group is a list of source and destination media access control (MAC) addresses seen in good packets promiscuously received from the LAN. Statistics included in this group include packets and octets sent and received by a given MAC address, and errors, broadcast packets, and multicast packets sent by a given MAC address.

HostTopN Group. The hostTopN group is used to prepare reports that describe the Ethernet hosts that top a list ordered by one of their statistics included in the host group over a specified time interval.

Matrix Group. The matrix group stores statistics for conversations between sets of two addresses. The statistics include a count of packets, octets, and errors. To facilitate easy retrieval of data by an SNMP management application, the group contains tables indexed by source/destination and by destination/source addresses.

Filter and Packet Capture Groups. The filter and packet capture groups work in conjunction to allow a method for easily and flexibly capturing a desired subset of the packets on the monitored LAN.

Alarm and Event Groups. The alarm group monitors variables in the probe and compares them to configured thresholds. If the monitored variable crosses a threshold, an event is generated. A hysteresis mechanism is implemented to limit the generation of alarms. Once again, this group is useful in reducing the SNMP traffic between the SNMP management application. The alarm group works in conjunction with the the event group that controls the generation and notification of events from the probe.

As described below, groups contained in the RMON-2 MIB include the protocol directory, protocol distribution, network layer host, network layer matrix, application layer host, application layer matrix, and user history groups.

Protocol Directory Group. This group identifies the protocols that the probe can monitor.

Protocol Distribution Group. This group contains statistics describing the number of packets and octets of each protocol detected on the monitored LAN.

Network Layer Host Group. This group contains statistics describing the number of packets and octets to and from each network address identified in packets detected on the monitored LAN.

Network Layer Matrix Group. This group contains statistics describing the number of packets and octets sent between pairs of network addresses

identified in packets detected on the monitored LAN. As with the Ethernet layer matrix group, to facilitate simple retrieval of data by an SNMP management application, the group contains tables indexed by source/destination and by destination/source addresses. In addition to the nlMatrixTable, the network layer matrix group also contains the nlMatrixTopNTable, which allows easy documentation of the network layer conversations generating the most traffic.

Application Layer Host Group. This group contains statistics describing the number of packets and octets of each protocol sent to and from each network address identified in packets detected on the monitored LAN. The application layer host group is not limited to protocols identified with layer 7 of the OSI network model (reference 6), but, in general, contains statistics for protocols from layers three through seven.

Application Layer Matrix Group. This group contains statistics describing the number of packets and octets of each protocol sent between pairs of network addresses identified in packets detected on the monitored LAN.

User History Group. The user history group provides a more general means than the Ethernet history group, of storing historical statistics on the probe. This group allows for identification of the time interval, the total length of time, and the variable to store. As with the Ethernet history group, the user history group reduces the required number of communications between an SNMP management application and the probe.

Through the design of the RMON and RMON-2 MIBs as described above, an RMON probe can provide a network manager with both real-time information, and with information gathered over prolonged collection periods. Typically, network managers use real time information for pro-active and fault management, while they typically use the information gathered over prolonged periods for performance management. A RMON/RMON-2 SNMP management application with a graphical user interface is desirable to effectively utilize the real-time information provided by the probe. A general-purpose SNMP utilities package and a general-purpose plotting package in combination with some simple scripts to sort out the data are the only requirements for collection and presentation of historical data. As will be detailed in section 4, during JWID 97, use was made of both real-time and historical information.

3. JWID 97 and COMPASS

The first part of this section provides general background on JWID 97 and COMPASS, and the role that COMPASS played in the demonstration. The end of this section summarizes the RMON-2 setup in the COMPASS lab.

JWID 97 was a United States and Allied Coalition operation led by the Commander, Carrier Group Six who acted as the Commander, Coalition Task Force (CCTF) conducting Combined Operations at the Joint Component Commander Level. There were many purposes for JWID 97, but most relevant to this report was the goal of demonstrating innovative telecommunications and information management technology that enhance data delivery to and from Joint Warriors, particularly common operational picture and imagery. Commander-in-Chief United States Atlantic Command (CINCUSACOM) was the host CINC operating from the Joint Battle Center (JBC) at the Joint Training Analysis and Simulation Center (JTASC) in Suffolk Virginia. The CCTF and his staff operated from USS *John C. Stennis* (CVN 74). JWID 97 took place from 7 July to 31 July 1997.

The U.S. Department of Defense's Defense Modeling and Simulation Office (DMSO) sponsored Command, Control, Communications, Computers, and Intelligence (C4I)-to-Simulation Initiative includes the Common Operational Modeling, Planning and Simulation Strategy (COMPASS). Goals of this C4I-to-SIM Initiative are to: (1) take Modeling and Simulation (M&S) to war and (2) train as you fight. Achieving such goals provides additional valuable information to operational planners. It gives them much greater insight and analysis from operational plans. Such goals enhance mission preview and rehearsal. They afford M&S resources an opportunity to collaborate with operational planners in their planning process, to gain more effective combat power for warfighters from improved plans.

The JWID 97 Coalition Wide Area Network (CWAN) backbone consisted of multiple T-1 lease lines and additional sites connected through the Defencse Information Systems Agency (DISA) Leading Edge (LES) Asyncronous Transfer Mode (ATM) network. Super High Frequency (SHF), Ultra High Frequency (UHF) and the Global Broadcast System (GBS) were used to extend the terrestrial backbone to mobile units and allied sites. The CWAN was a U.S. Secret-with-allied-releasable network, and was a separate network from the existing Non-Classified IP Routing Network (NIPRNET) and Secret IP Routing Network (SIPRNET). Network Encryption System (NES) from Motorola was used to secure the information carried over the T-1 lease lines between major backbone sites.

NRaD was one of the secondary sites in the CWAN. NRaD was connected to the CWAN through a T-1 lease line to the Naval Telecommunications Center LANT in Hampton Roads, VA (NH95). NRaD was also connected to Naval Computer and Telecommunications Area Master Station EASTPAC in Wahiawa, HI (Wahiawa) through another T-1 lease line. The connection to Wahiawa provided the USS *Coronado*, Aus-

tralia, and New Zealand access to the CWAN. NRaD also provided multicast e-mail service to the Multi-National Task Group (MNTG) through a UHF broadcast channel.

The existing Timeplex network connected sites local to NRaD, including the COMPASS lab, the Joint Maritime Communications System (JMCOMS), and the Reconfigurable Land-Based Test Site (RLBTS), to the CWAN. KIV-7 and KG-194 cryptos were used to protect the data. The portion of the CWAN local to NRaD was a full-function network with its own domain <nrad.jwid.cmil.mil> and its own address block and services, including e-mail and domain name service (DNS).

COMPASS participated in JWID 97 in order to demonstrate its capabilities and allow the warfighter to evaluate this technology during a simulated conflict. COMPASS-capable workstations were deployed to all major JWID sites, including numerous secondary sites. Since the COMPASS lab at NRaD has many communications channels available, the lab was selected to host the NRaD Coalition Wide Area Network (CWAN) presence and to serve as a communications node on the CWAN. COMPASS utilized the T-1 link to NH95 to receive data over the CWAN from the East Coast, the T-1 link to Wahiawa to connect the CWAN to our Allies in New Zealand and Australia, a 64kb feed to JMCOMS for further distribution over SATCOM to ships at sea, and a 256kb feed to RLBTS acting as a site. Figure 1 shows the JWID sites relevant to this report. The NH95, Wahiawa, and JMCOMS sites were essentially communications hubs through which COMPASS related traffic was routed to other locations. Note that for the purposes of this report the figure depicts the COMPASS lab as being the central JWID site, which was not the case from a more general perspective. For a more detailed and complete description of the JWID 97 CWAN, refer to reference 7.

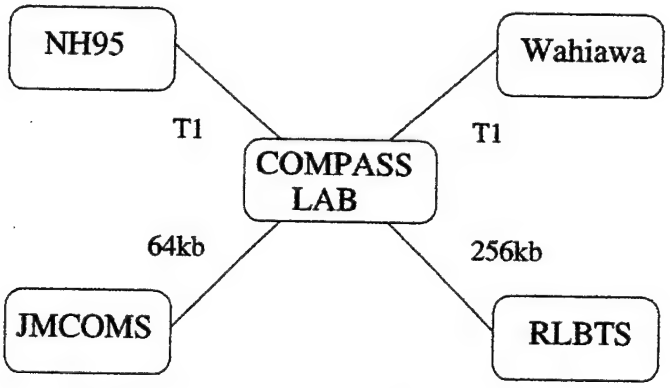

Figure 1. COMPASS connectivity to various JWID sites.

COMPASS enhancements added several COTS, public domain, and government off-the-self (GOTS) tools to the applications. The GOTS software was comprised of the COMPASS servers and the COMPASS client software embedded in the host application. The COMPASS servers, located at NRaD, received data from simulation applications (e.g., Extended Air Defense Simulation (EADSIM)) and then sent the required updates to the various COMPASS clients at each of the JWID sites. The COTS

tools were comprised of the Sun Micro Systems *Showme* white-board application, the Netscape Web browser, and a "chat" application call *Global Chat.* Public domain software included three standard Multicast Backbone (M-Bone) applications, an audio application called *Visual Audio Tool*, a video application called *Network Video*, and the *Session Directory* application used to provide a listing of active multicast sessions and to enable users to join a multicast session. The COMPASS client/server traffic and the white-board application were the primary sources of unicast traffic. In order to support the audio and video tools, M-bone multicast routing daemon software was added to selected workstations to create a system of multicast tunnels from site to site. The multicast applications sent out multicast packets that were received by the multicast servers, encapsulated in unicast packets, and sent to the appropriate multicast servers. Upon reception of the tunneled traffic, the receiving multicast server extracted and sent out the encapsulated multicast packets to be received by the workstations hosting the appropriate applications. The traffic associated with these multicast tunnels was carefully examined in this study.

A RMON-2 probe was placed on the LAN local to the COMPASS lab in NRaD Building 40. By using a COTS RMON-2 SNMP management application called Meterware (reference 4), real-time information from the probe was utilized by network managers for pro-active and fault management. Meterware was installed on a PC also located on the LAN local to the COMPASS lab, so the substantial amount of traffic generated between Meterware and the probe did not create a congestion problem. Besides providing a display of real-time data, Meterware was also configured to collect and store some historical information, most notably data documenting the amount of traffic detected for each protocol. In addition to the historical data collected by Meterware, additional data were periodically collected. The nlMatrixTopNTable was configured to record the top 150 network-layer conversations in 30-minute intervals, and scripts using general SNMP utilities hosted on a UNIX workstation were scheduled to periodically collect this information. As stated in the previous paragraph, the multicast applications communicating between the NRaD COMPASS lab and the other JWID 97 sites were a primary focus of this investigation. Because of the limited bandwidth between COMPASS and these other sites, and because this bandwidth would be even more limited in a true operational environment, documentation of the the tunneled multicast traffic between the various sites was considered a priority. Therefore, scripts using general SNMP utilities were scheduled to periodically collect information from the nlMatrixSDTable (using source-destination indexing) relevant to the network layer traffic originating from the multicast server in the COMPASS lab, and information from the nlMatrixDSTable (using destination-source indexing) relevant to the network layer traffic received by the multicast server in the COMPASS lab.

4. RESULTS

The results of the implementation of RMON technology for COMPASS during JWID 97 are divided into two sections. A brief section describing the operational benefits provided by the RMON probe precedes a longer section describing the historical data collected with the probe.

4.1 OPERATIONAL

Because of the network topology described in section 3, during the demonstration it was crucial that network managers be able to identify the sources of excessive traffic traveling between the COMPASS lab and the other participating sites. Less granular information, such as total number of packets in and out of a gateway router can easily be monitored with standard network management utilities, but an RMON probe is required to quickly identify a particular host that is generating too much traffic. Figure 2 shows one of the Meterware displays.

The matrix information display shown in figure 2 was particularly useful for the network managers. On the left side of the display is a list of protocols that one can select. Typically, IP was the protocol selected for display. On the top right-hand side of the display is a tabular listing of the network layer conversations generating the most traffic of the selected protocol. On the bottom right is a graphical view of this tabular information. Meterware allows for updates of these data on demand, giving the network manager real-time information on hosts generating traffic of particular protocols. Therefore, for instance, when a multicast server at one of the remote JWID sites was tunneling an excessive amount of traffic to the COMPASS lab, a network manager use the Meterware display to quickly identify the remote multicast server and the host of the originating application, allowing the network manager to notify the culprit of the problem. Similarly, if one of the applications running in the COMPASS lab was generating too much multicast traffic, which was subsequently routed over a low-bandwidth connection to one of the other JWID sites, that application could be quickly identified, and the problem corrected. As will be seen in the next section, the use of the RMON-2 probe in combination with other network management resources resulted in identification of problems in the multicast tunnel configuration. Modifications of the configuration were made during the testing period, resulting in a significant reduction in traffic on the links between the COMPASS lab and the other JWID sites.

4.2 HISTORICAL

It was desired to obtain some measure of the traffic sent between the COMPASS lab and the other JWID 97 sites. To this end, at the conclusion of the JWID 97 demonstration, scripts were written to sort and manipulate the data collected from the nlMatrixTopNTable, nlMatrixDSTable and nlMatrixSDTable. The relevant conversations included in the data collected from the nlMatrixTopNTable were summed

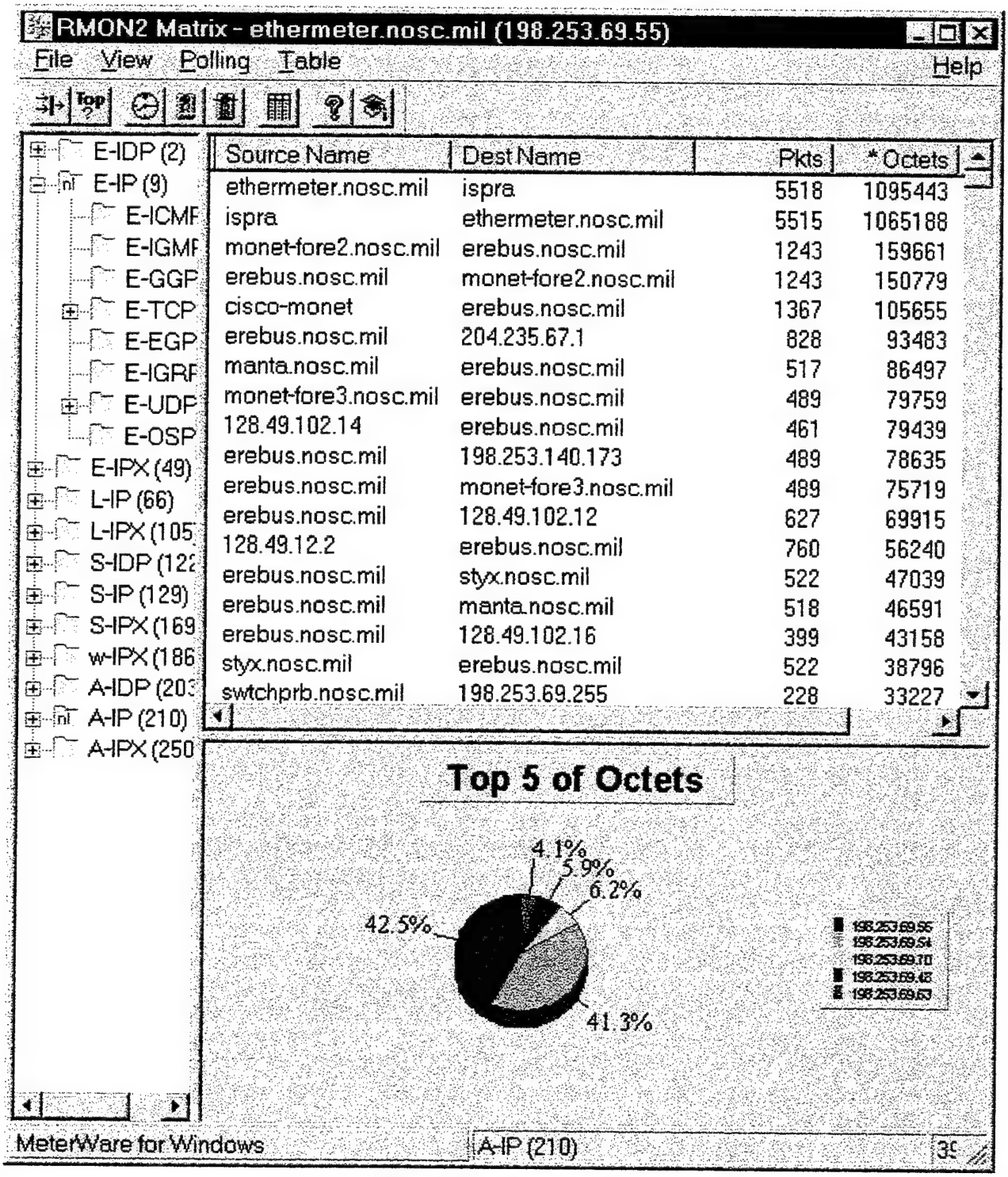

Figure 2. A Meterware display.

so as to yield plots of the IP traffic to and from the COMPASS lab and the various other JWID sites. These plots are presented in figures 3 through 10. Only data during the testing periods, 0700-2230 EDT, weekdays from 15 July through 31 July 1997, are shown in the plots. Since these plots depict data extracted from the top 150 IP conversations, the results are an approximation, where the true octets rates were higher. For the Wahiawa, NH95, and RLBTS data, this error is insignificant. This can be deduced from the JMCOMS data, figures 9 and 10, where it is seen that conversations exchanging very few packets were included in the top 150 IP conversations. Since it is known that there were not an extremely large number of conversations, each exchanging small amounts of traffic, it follows that Wahiawa, NH95, and RLBTS would not be significantly changed by data that were not included in the top 150 IP conversations. On a relative scale, there may be larger errors in the JMCOMS data, but on an absolute scale, the results show that only a small of traffic was exchanged between COMPASS and JMCOMS. The small amount of traffic to COMPASS is partly a result of the 64kb link from the COMPASS lab to JMCOMS, but more so because data sent to JMCOMS were then passed over even narrower bandwidth RF links to simulated ships and ships at sea.

Figures 3 through 10 indicate that significantly more traffic was sent by the COMPASS lab to RLBTS and Wahiawa than was sent from RLBTS and Wahiawa to the COMPASS lab, and somewhat more traffic was sent by the COMPASS lab to NH95 than from NH95 to the COMPASS lab. This was true because the COMPASS servers were usually located at the COMPASS lab. When data were received from a single COMPASS client, the required updates were unicast from the COMPASS servers to all COMPASS clients at the various JWID sites. In addition, much of the multicast traffic, detailed further in the following paragraphs, was generated by applications residing in the COMPASS lab and at sites that routed traffic through NH95, whereas RLBTS and sites routing traffic via Wahiawa generated little multicast traffic.

The tunneled multicast traffic exchanged between the multicast server in the COMPASS lab and the multicast servers at the other sites was of primary interest to the COMPASS effort. Therefore, data for individual multicast server to multicast server conversations collected from the nlMatrixDSTable and nlMatrixSDTable were summed appropriately so as to yield plots of the total amount of traffic between the multicast servers at the various JWID 97 sites. Note that these data are the total IP traffic between the multicast servers, and are not limited to the tunneled multicast traffic between the servers. Unfortunately, the RMON-2 probe used did not yet support the limited protocol extensibity as described in the RMON-2 standard, therefore it was not possible to distinguish between traffic exchanged on the multicast tunnel TCP port and other TCP traffic. Because there were no other network applications regularly communicating between the the multicast servers, it can be safely assumed that the vast majority of traffic between the multicast servers was, in fact, tunneled multicast traffic.

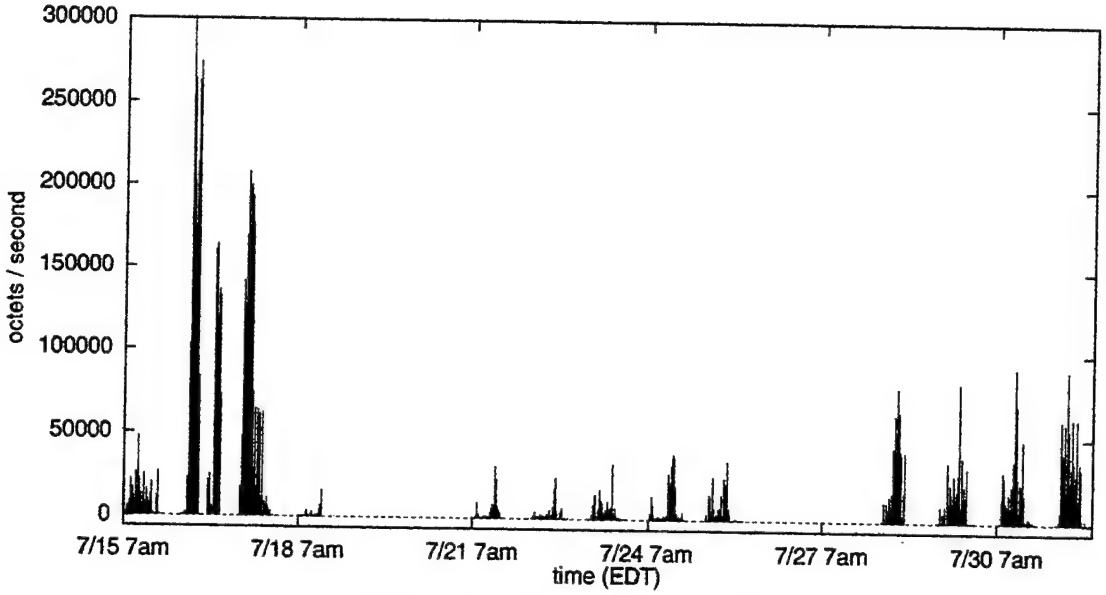

Figure 3. Traffic during the testing period from the COMPASS lab to NH95.

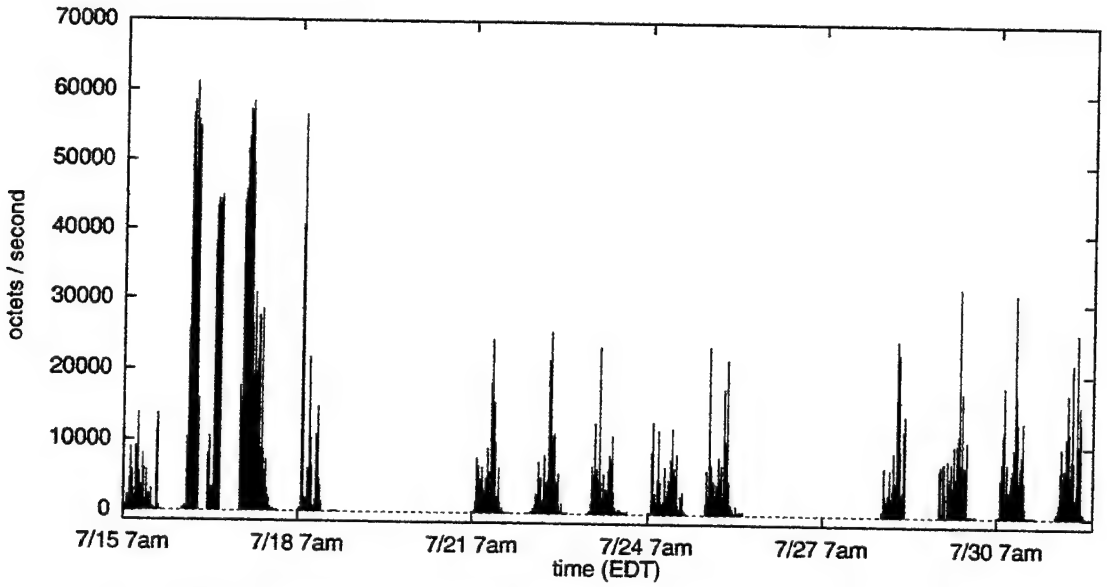

Figure 4. Traffic during the testing period from NH95 to the COMPASS lab.

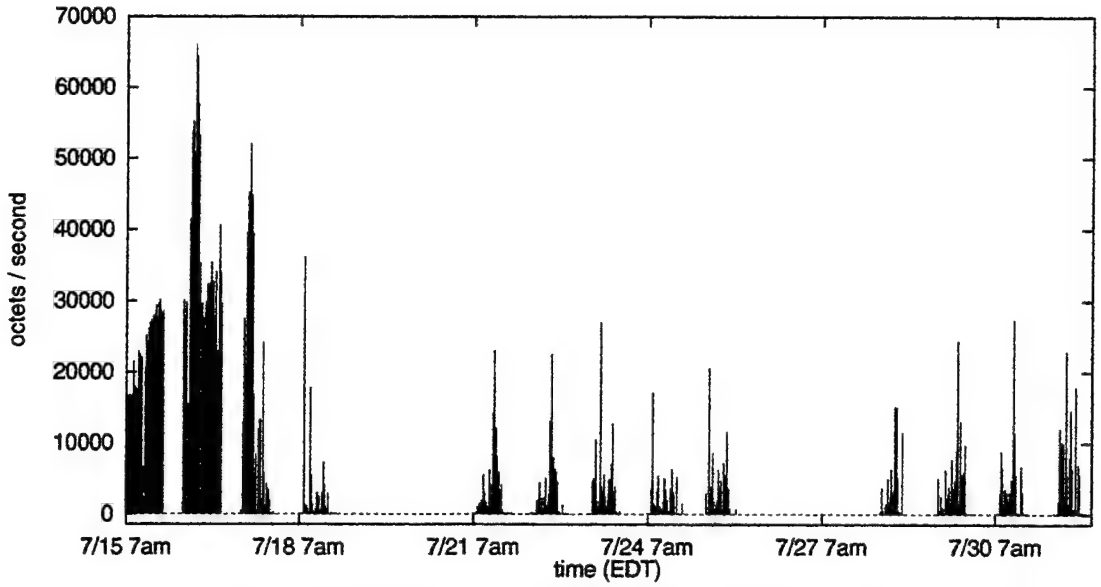

Figure 5. Traffic during the testing period from the COMPASS lab to RLBTS.

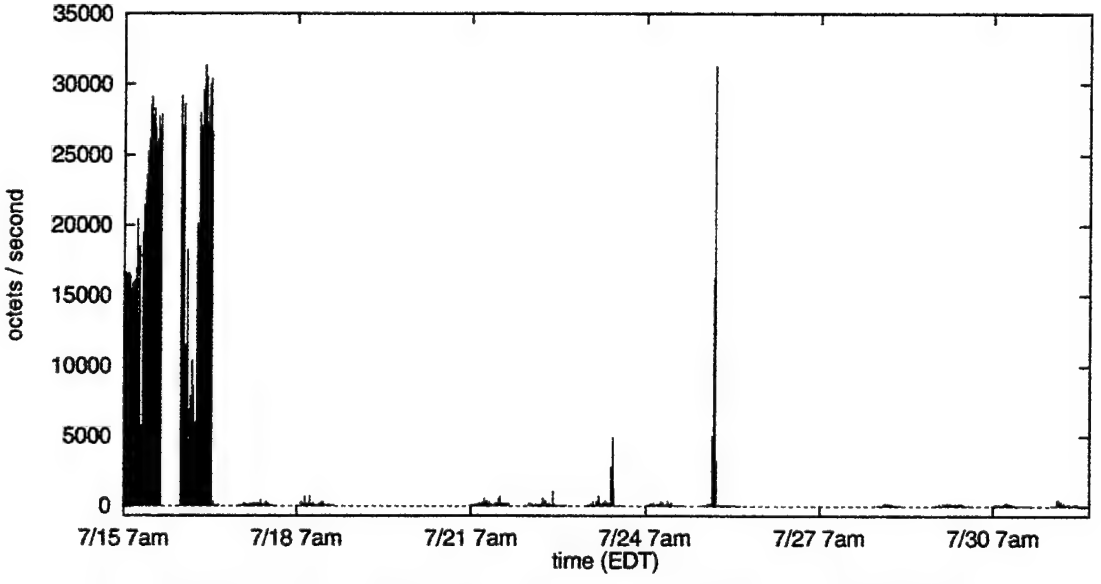

Figure 6. Traffic during the testing period from RLBTS to the COMPASS lab.

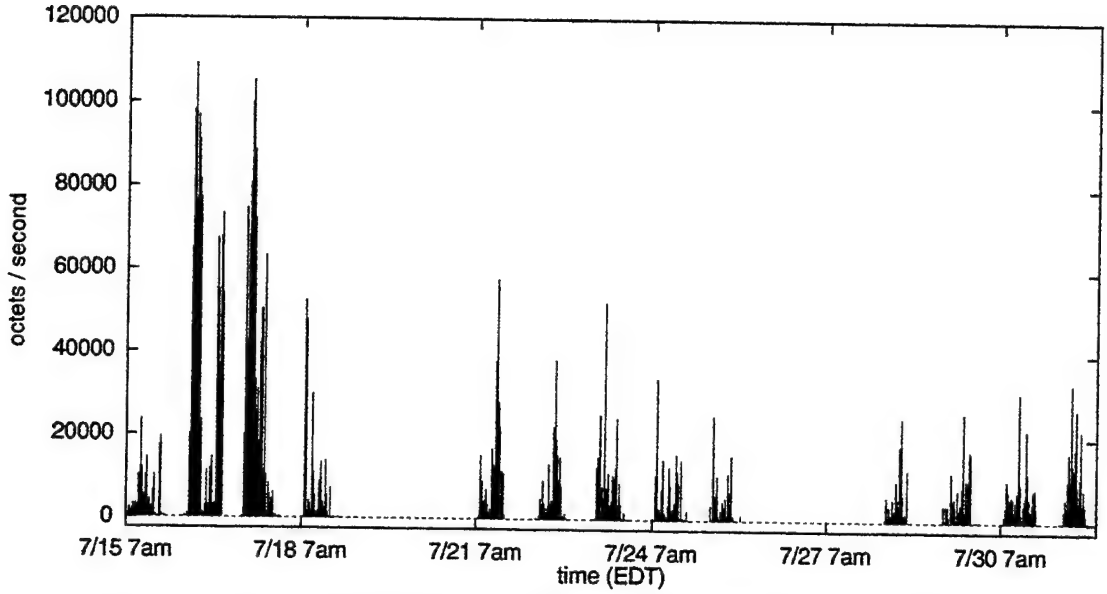

Figure 7. Traffic during the testing period from the COMPASS lab to Wahiawa.

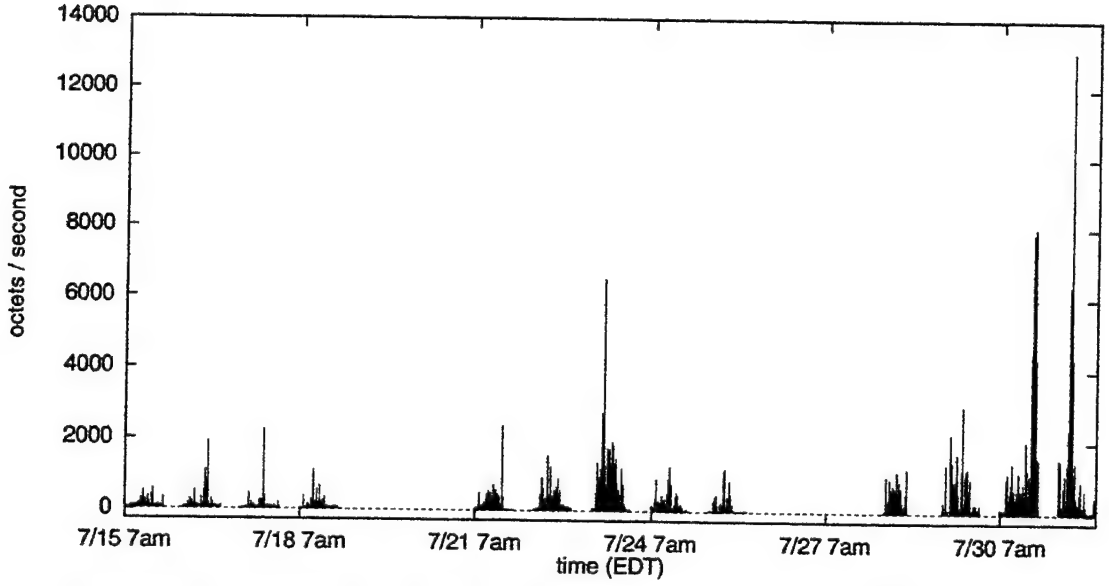

Figure 8. Traffic during the testing period from Wahiawa to the COMPASS lab.

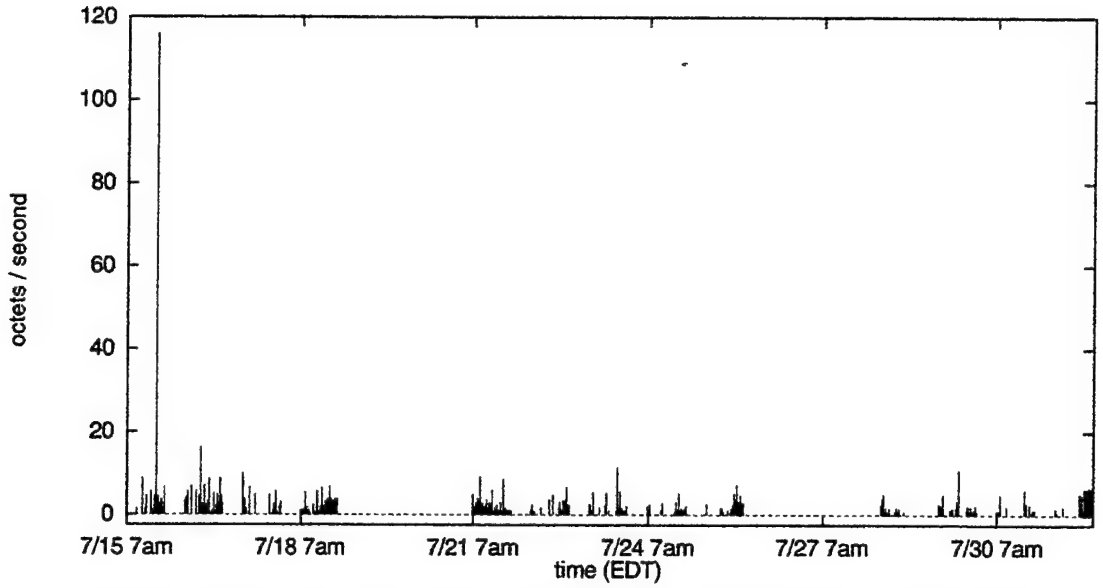

Figure 9. Traffic during the testing period from the COMPASS lab to JMCOMS.

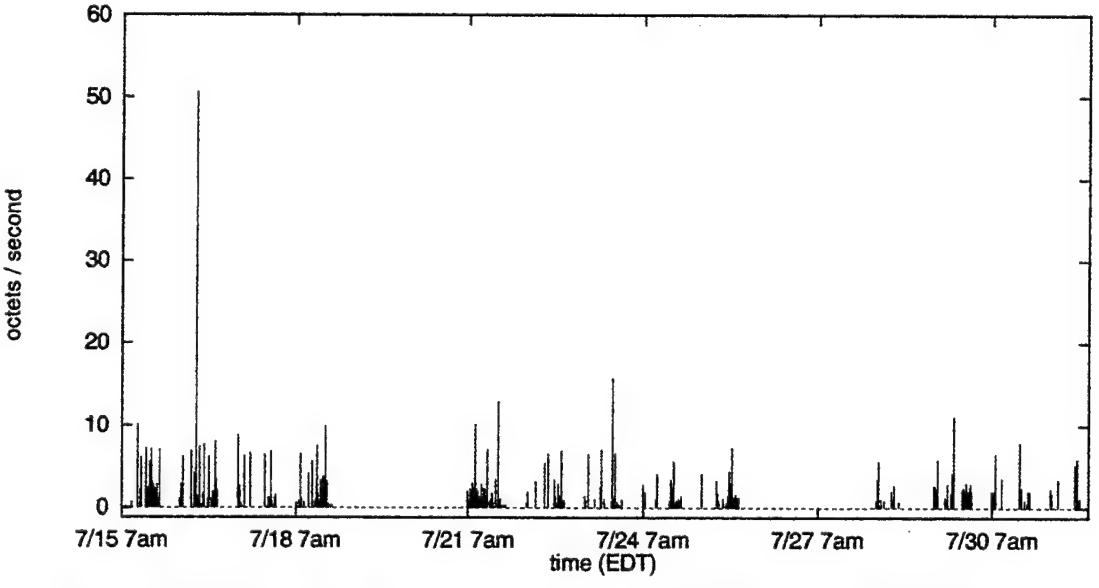

Figure 10. Traffic during the testing period from JMCOMS to the COMPASS lab.

The results of the multicast server traffic are shown in figures 11 through 16. For tunneled traffic originating from the COMPASS lab, data for the entire period from 16 July 1415 EDT through the end of July are shown in the plots. For tunneled traffic coming into the COMPASS lab, data for the entire period from 17 July 1915 EDT through the end of July are shown in the plots. Figures 11, 13, and 15 indicate that on 17 July, significantly more multicast traffic was tunneled from the COMPASS lab as compared to the subsequent days. This high level of traffic on 17 July (and before 17 July, as illustrated in figures 3 through 8) was caused by the original configuration of the multicast tunnels wherein the multicast server in the COMPASS lab was acting as a hub for all multicast traffic. This configuration was modified so that multicast traffic was routed to the COMPASS lab only when necessary. The figures indicate that significantly more multicast traffic was sent by the COMPASS lab to RLBTS and Wahiawa than from RLBTS and Wahiawa to the COMPASS lab. Once the multicast tunnel configuration was modified, the COMPASS lab and NH95 sites exchanged similar amounts of multicast tunnel traffic.

Figures 11 through 16 can be compared with figures 3 through 8 to gain insight into the relative amount of tunneled multicast traffic between the sites as compared with the total traffic. A comparison between figures 5 and 13 and between figures 7 and 15 suggests that much of the traffic from COMPASS to RLBTS and Wahiawa was tunneled multicast traffic. Figures 3 and 11 indicate that there was a significant amount of traffic sent from COMPASS to NH95 that was not multicast tunneled traffic. This is at least in part explained by figure 17, which shows the IP traffic sent from the two main COMPASS servers in the COMPASS lab to NH95. It is seen that due to the numerous COMPASS clients routing traffic through NH95, a significant amount of unicast traffic was sent from the COMPASS servers through NH95.

There are several instances where it appears that there was more traffic indicated in the multicast data than in the topN data. This is because these data points occurred outside the testing period, which is not shown in the topN figures.

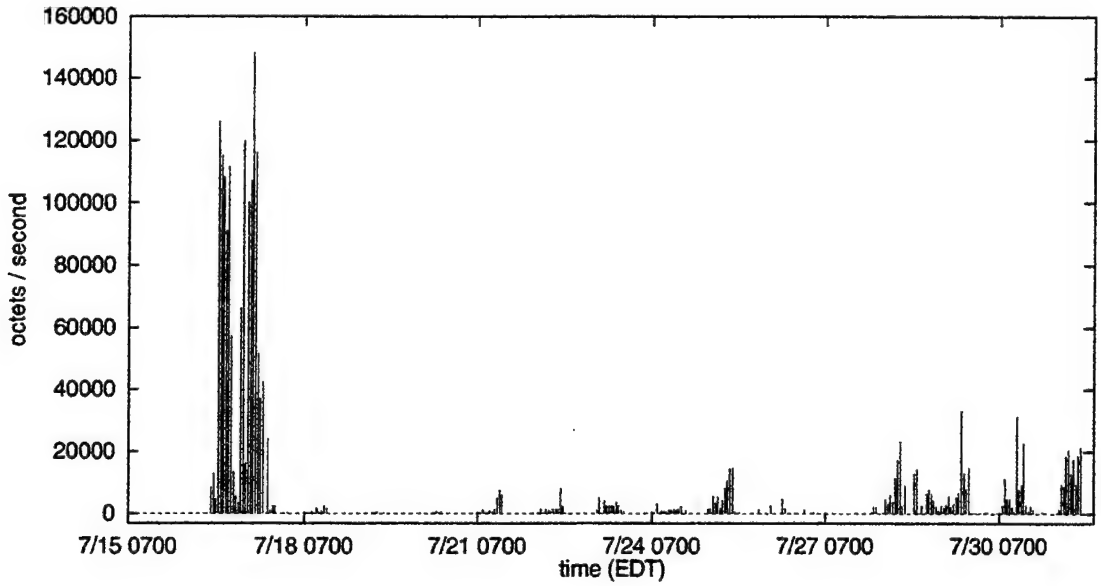

Figure 11. Multicast server traffic from COMPASS lab to NH95. Data collection started on 16 July at 1415 EDT.

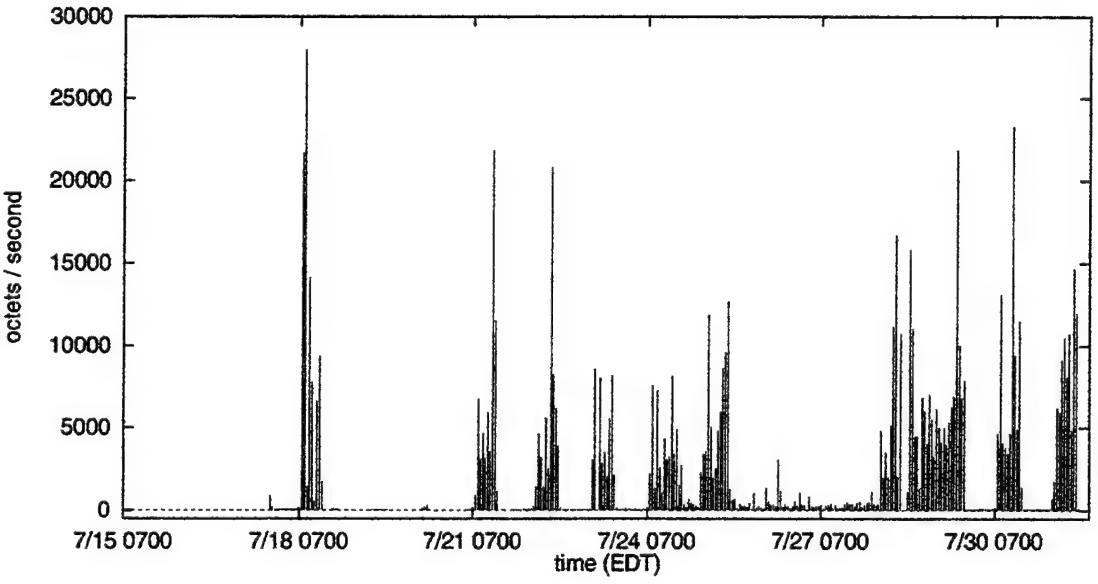

Figure 12. Multicast server traffic from NH95 to the COMPASS lab. Data collection started on 17 July at 1915 EDT.

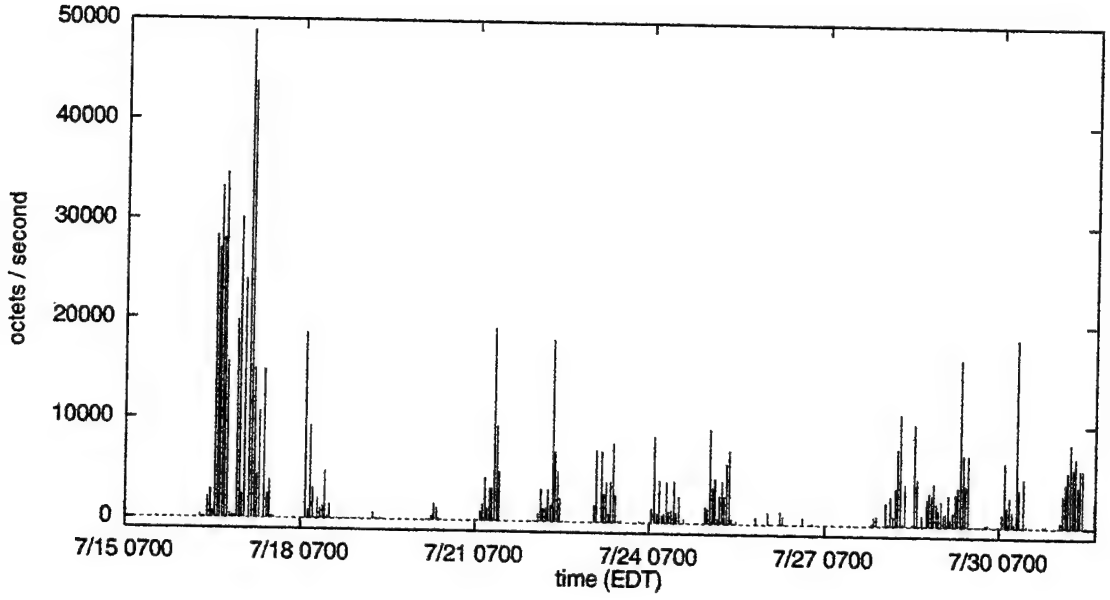

Figure 13. Multicast server traffic from COMPASS lab to RLBTS. Data collection started on 16 July at 1415 EDT.

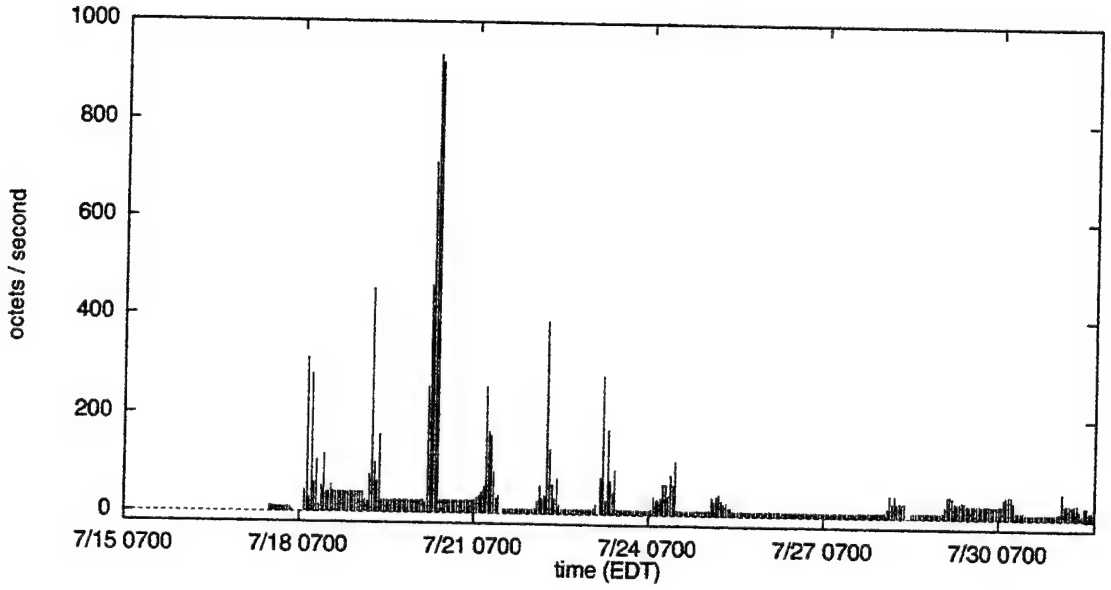

Figure 14. Multicast server traffic from RLBTS to the COMPASS lab. Data collection started on 17 July at 1915 EDT.

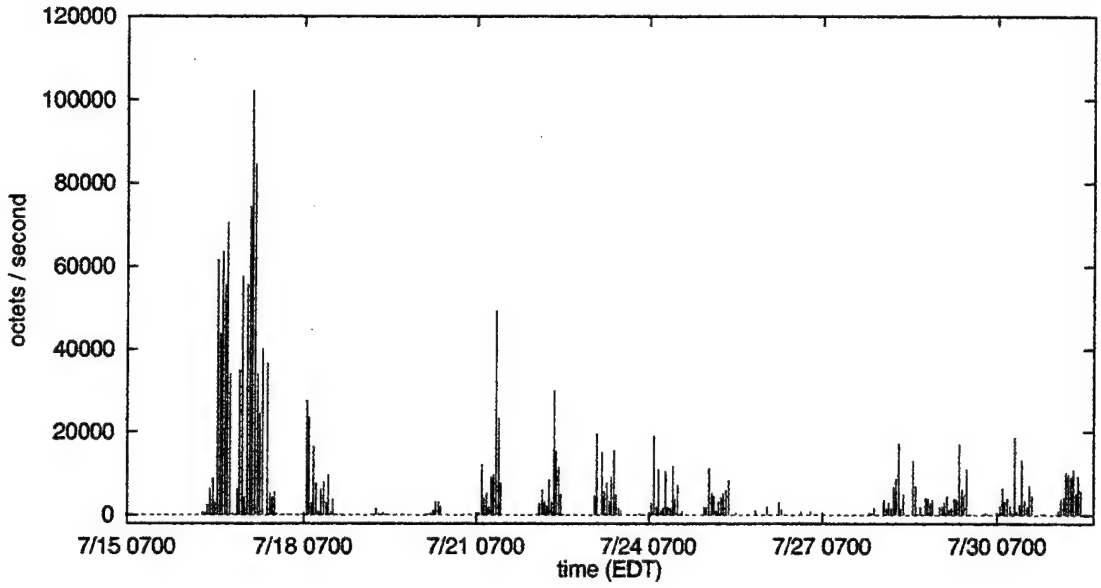

Figure 15. Multicast server traffic from COMPASS lab to Wahiawa. Data collection started on 16 July at 1415 EDT.

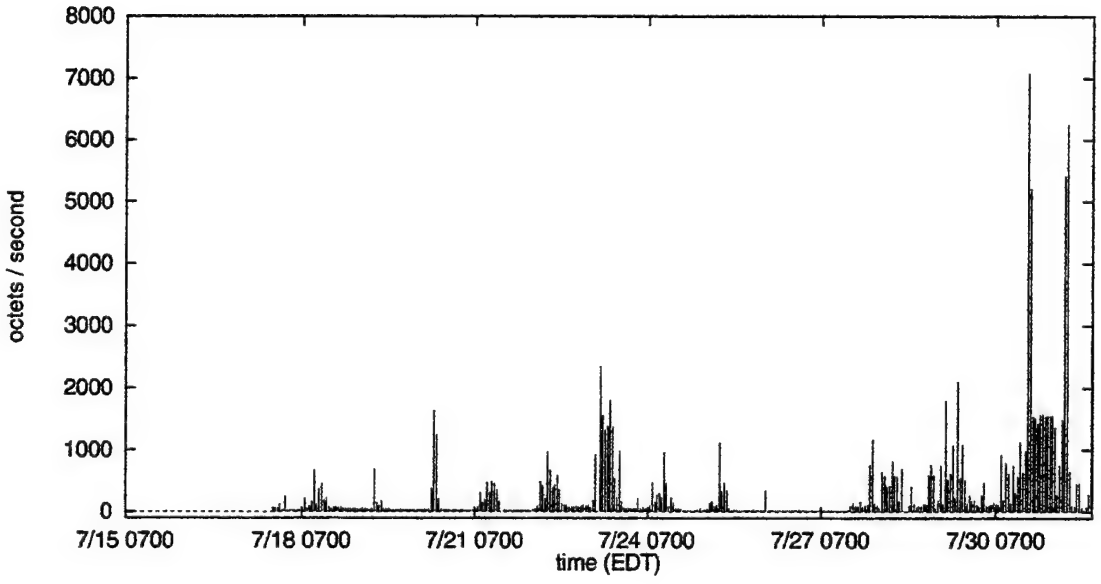

Figure 16. Multicast server traffic from Wahiawa to the COMPASS lab. Data collection started on 17 July at 1915 EDT.

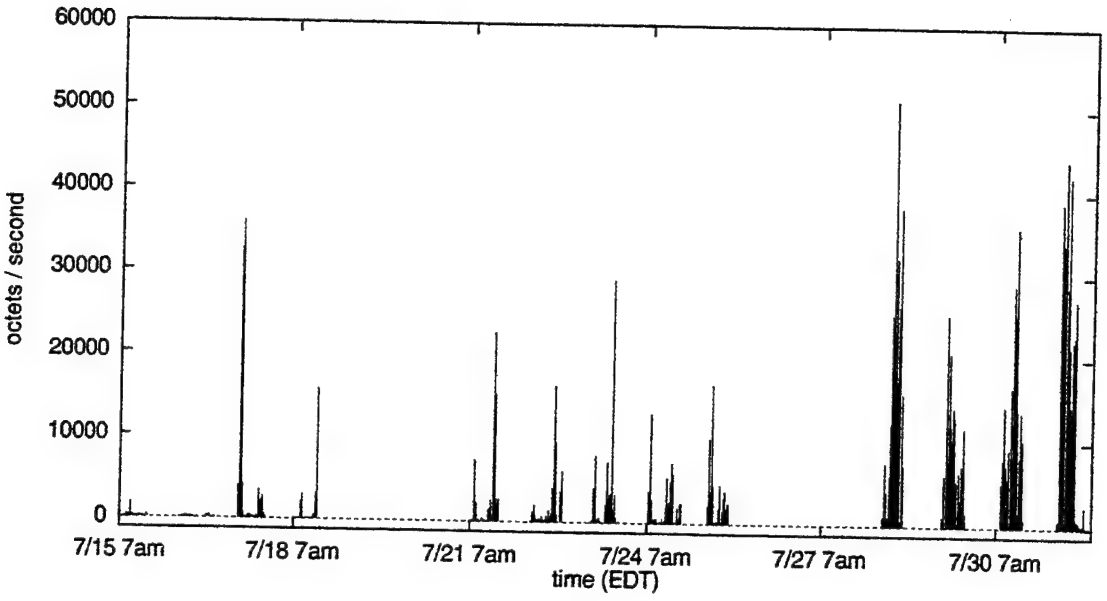

Figure 17. Unicast traffic during the testing period from the two COMPASS servers to NH95.

5. SUMMARY AND CONCLUSION

This report documents the results obtained from implementation of RMON-2 technology in the NRaD COMPASS lab during JWID 97. The RMON-2 technology was utilized for operational network management and to collect historical data for review of network utilization during the demonstration.

The operational utilization RMON-2 was successful. The real-time information obtained from the RMON-2 probe and displayed using COTS software proved to be a necessary aid for network managers in maintaining desired network performance. This was best demonstrated by the reconfiguration of multicast tunnels during the test, thereby reducing the traffic on the links between the COMPASS lab and other JWID sites to acceptable levels. Utilization of RMON-2 for collection of historical data was also successful. Data collected over the demonstration period documented the amount of traffic (octets and packets), the type of traffic (link layer through application layer protocols), and the source and destination of traffic (link and network layer addresses).

For the purposes of the COMPASS lab participation in JWID 97, historical data collection documented network utilization during the demonstration. In particular, the statistics gathered on the tunneled multicast traffic and the traffic from COMPASS servers may help explain the network requirements for COMPASS in future scenarios. The type of historical data obtained during the demonstration would help optimize network performance in scenarios where the relevant networks will operate over extended time periods.

It is anticipated that the successful implementation of RMON-2 in this demonstration will be a stepping stone towards the utilization of this technology in the operational environment.

6. REFERENCES

1. S. Waldbusser. 1995. "Remote Network Monitoring Management Information Base," RFC1757.

2. S. Waldbusser. 1997. "Remote Network Monitoring Management Information Base Version 2 using SMIv2," RFC2021.

3. K. McCloghrie, M. Rose. 1991. "Management Information Base for for Network Management of TCP/IP-based Internets: MIB-II," RFC1213.

4. Technically Elite, Inc., San Jose, CA. http://www.tecelite.com/index.html

5. M.T. Rose. 1994. *The Simple Book, An Introduction to Internet Management*, P T R Prentice Hall, Englewood Cliffs, NJ.

6. J. D. Day and H. Zimmerman. 1983. "OSI Reference Model," *Proceedings of the IEEE*, vol. 71, pp. 1334–1340.

7. Defence Information Systems Agency. "Joint Warrior Interoperability Demonstration," http://www.jwid.disa.mil/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1997	Final: August 1997

4. TITLE AND SUBTITLE

RMON-2 IMPLEMENTATION AND RESULTS FOR COMMON OPERATIONAL MODELING, PLANNING, AND SIMULATION STRATEGY DURING JWID 97

5. FUNDING NUMBERS

PE: 0603794N
AN: DN306547
WU: X2091

6. AUTHOR(S)

E. W. Jacobs, L. M. Gutman, R. H. Cheng, M. S. Lavelle

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Command, Control and Ocean Surveillance Center (NCCOSC)
RDT&E Division (NRaD)
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

TR 1753

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Space and Naval Warfare Systems Command
Washington, D. C. 20363–5100

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This report documents the results obtained from Remote Monitoring (RMON) technology in the Naval Command, Control and Ocean Surveillance Center (NCCOSC) RDT&E Division (NRaD) Common Operational Modeling, Planning, and Simulation Strategy (COMPASS) lab during the 1997 Joint Warrior Interoperability Demonstration (JWID 97). The report reviews the essentials of RMON and RMON-2 technology and describes COMPASS lab participation in JWID 97. The report then discusses the results of utilization of RMON-2 for operations and for historical data collection.

14. SUBJECT TERMS

Mission Area: Command, Control, and Communications
operational network management
Common Operational Modeling, Planning, and Simulation Strategy (COMPASS)
historical data collection
Joint Warrior Interoperability Demonstration (JWID)

15. NUMBER OF PAGES

31

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS REPORT

21a. NAME OF RESPONSIBLE INDIVIDUAL	21b. TELEPHONE *(include Area Code)*	21c. OFFICE SYMBOL
E. W. Jacobs	(619) 553-1614 e–mail: jacobs@nosc.mil	Code D364

INITIAL DISTRIBUTION

Code D0012	Patent Counsel	(1)
Code D0271	Archive/Stock	(6)
Code D0274	Library	(2)
Code D027	M. E. Cathcart	(1)
Code D0271	D. Richter	(1)
Code D364	E. W. Jacobs	(10)
Code D7211	J. W. Novotny	(1)
Code D805	M. S. Kvigne	(1)
Code D82	R. J. Kochanski	(1)
Code D827	C. W. Warner	(1)
Code D827	L. W. Gutman	(1)
Code D827	R. H. Cheng	(1)
Code D8405	B. J. Marsh	(1)
Code D8405	R. D. Peterson	(1)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (4)

NCCOSC Washington Liaison Office
Arlington, VA 22245–5200

Center for Naval Analyses
Alexandria, VA 22302–0268

Navy Acquisition, Research and Development
Information Center (NARDIC)
Arlington, VA 22244–5114

GIDEP Operations Center
Corona, CA 91718–8000